CLAIMS

What is claimed is:

1. A token, comprising:

an identification number encoded on the token and a private key stored in the token; and

a plurality of certificates/private keys wrapped in a public key which may be activated by the private key on the token with the entry of a passphrase.

2. The token recited in claim 1, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key.

3. The token recited in claim 2, wherein the wrapping of the certificates/private keys with the token public key encrypts the certificates/private keys.

4. The token recited in claim 3, wherein the token is a smart card.

5. A method of revoking a token, comprising:

accessing a database having a plurality of records accessible by user identification and token identification, wherein said database has a plurality certificates/private keys associated with each token identification;

revoking each certificate/private key associated with a selected token identification for a given token.

6. The method recited in claim 5, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key

7. The method recited in claim 6, wherein the token is a smart card.

8. The method recited in claim 7, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

9. A method of updating a token, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys in the download packet using the private key in the token.

10. A method as recited in claim 9, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid form the token.

11. The method recited in claim 10, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

12. The method recited in claim 11, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key

13. The method recited in claim 12, wherein the token is a smart card.

14. A computer program embodied on a computer readable medium and executable by a computer for revoking a token, comprising:

accessing a database having a plurality of records accessible by user identification and token identification, wherein said database has a plurality certificates/private keys associated with each token identification;

revoking each certificate/private key associated with a selected token identification for a given token.

15. The computer program recited in claim 15, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key

16. The computer program recited in claim 15, wherein the token is a smart card.

17. The computer program recited in claim 16, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

18. A computer program for updating a token embodied on a computer readable medium and executable by a computer, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private

keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys using the private key in the token.

19. The computer program as recited in claim 18, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid from the token.

20. The computer program recited in claim 19, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

21. The computer program recited in claim 20, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key

22. The computer program recited in claim 21, wherein the token is a smart card.